NASA OIG Review

May 1999
Vol 1. No. 1

NASA OIG Review is distributed to Congress, NASA, and other government agencies to provide information about the reports and activities of the NASA Office of Inspector General

New Reports!

RECOVERING FROM DISASTER

The OIG is conducting a series of audits to determine whether selected NASA and contractor programs are adequately prepared to continue computing operations in the event of a disaster. We recently issued reports about disaster recovery at Johnson Space Center (Johnson) and JPL. We reported on disaster recovery at Goddard Space Flight Center in FY98 (*Report IG-98-036*) and audits are ongoing at Kennedy Space Center, Marshall Space Flight Center, and the Ames Research Center.

At Johnson (*Report IG-99-005*), we found that the Shuttle Software Production Facility has a disaster recovery plan, but the plan is not tested annually and the facility has no strategy or procedures in place for extended backup operations in the event of a disaster. Johnson responded adequately to many of our recommendations and we requested that they reconsider their position on the remainder.

At JPL (*Report IG-99-006*), we found that the emergency response contingency plan for the Telecommunications and Mission Operations Directorate, which supports space exploration missions, was missing important elements, and personnel were not following all of the plan's guidelines. As a result, the organization may not be prepared to provide mission-critical support in the event of a disaster. Management has agreed to follow our recommendations to improve contingency planning.

THE "RUSSIAN CHARTER"

NASA's Johnson Space Center was using a chartered DoD 727 aircraft to transport employees working on the space station project between the United States and Russia. The charter was intended to result in cost savings and programmatic benefits.

An inspections team determined that the charter service was not cost effective compared to commercial air services. In a final report *(Report G-98-014)*, we also highlighted concerns about the charter's physical security, procedures, and adherence to NASA transportation regulations. We found that programmatic considerations were insufficient to justify continuing the charter service.

NASA concurred with our single recommendation and terminated the charter service. This will result in cost savings to the government of approximately $4 million per year.

LESSONS LEARNED FROM MIR

During the Shuttle/ Mir Program, NASA astronauts spent almost two years living and working aboard the Russian Space Station Mir. During these visits, NASA gained experience working with the Russians in conducting experiments, repairing station systems, and responding to emergency situations. The "lessons learned" on Mir that could be applied to the International Space Station (ISS) program became one of NASA's main justifications for continuing the Shuttle/Mir program.

We reviewed the ISS Program implementation of the lessons acquired during the Shuttle/Mir program *(Report G-98-012)*. Our review concluded the process had been initiated late by the ISS Program, but the transfer of knowledge and experience was being adequately addressed. We discovered, however, that NASA was not adequately considering lessons learned during other U.S. and international long-duration space flights.

The Office of Space Flight agreed with our recommendations to identify points of contact for each lesson learned and to ensure the process of implementing lessons learned continued. However, they have not yet agreed with our recommendation to apply lessons learned from other long-duration missions to the ISS program.

Investigations

The OIG's investigative arm conducts criminal and regulatory investigations in which NASA is a victim. Recent OIG investigations led to the following results:

Canadian Hacker Charged

A Canadian citizen was held over for trial on forty-seven counts of illegal intrusions and hacking related to NASA sites. The hacker illegally penetrated and denied public access to the network server housing the NASA World Wide Web home page. He further altered the NASA home page by substituting a Hacker Manifesto in its place. The attack caused a denial of service to about 210,000 users attempting to access this page, and cost NASA tens of thousands of dollars to repair and secure the hacked systems. The OIG considers preserving and protecting NASA information a top priority.

Contractor Settles Over False Claims

A contractor paid $214,462 to the U.S. Treasury as part of a Release and Settlement Agreement with NASA. The Agreement reported that during the period 1992-1996, the company submitted 98 false claims to NASA. The false claims were based on "pro forma" invoices and payments to subcontractors prior to the actual delivery of services and materials. By paying the company in advance of the services being rendered, NASA lost use of its finances. The company received an "unjust enrichment" by using funds they were not yet entitled to.

Contractor Pleads Guilty

A Canadian corporation pled guilty to a conspiracy charge for misrepresenting the origin of Taiwanese-made strainers imported into the U.S. for use by NASA and the U.S. Navy. These strainers were installed on a high-pressure valve system at a NASA facility. NASA relies on the certifications provided by the corporation to insure the integrity of the equipment the parts are used on. The substitution of inferior or uncertified parts could cause catastrophic damage to NASA projects and serious injury to NASA employees. The OIG will continue to place safety its number one priority.

Guilty Plea on Kickback Charge

A former NASA contractor employee pled guilty to one count of conspiracy to violate the Anti-kickback Act of 1986, and one count of filing a false tax return concerning unreported income. He admitted receiving kickbacks from several NASA and Department of Defense subcontractors. He was sentenced to six months home confinement, ordered to pay a $3,000 fine, and directed to pay NASA $40,121 in restitution. Violations of the Anti-Kickback Act impact the basic integrity of the procurement process. This type of violation usually involves a subcontractor paying kickbacks to a prime contractor employee in a position to influence the award of subcontracts. The subcontractor then inflates his prices to recoup his kickback or supplies cheaper inferior materials to maintain a significant profit margin.

SPECIAL REPORT
Export Control

Theft of U.S. technological information by foreign entities has become a high profile issue following claims that launch vehicle technologies were leaked to foreign nations and nuclear secrets were stolen from Department of Energy laboratories. We recently evaluated NASA's protection of technologies subject to export control.

The resulting report, *NASA Control of Export-Controlled Technologies* (Report #IG-99-020), found that NASA has not identified all export-controlled technologies related to its major programs and does not maintain a catalog of classifications for transfers of export-controlled technologies. Also, Agency oversight and training of personnel in the Export Control Program needs to be improved. As a result, NASA may not have adequate control over export-controlled technologies to preclude unauthorized or unlicensed transfers.

We recommended that the Office of External Relations develop policies and procedures to ensure that:

- all export-controlled technologies are identified and protected
- only qualified personnel perform export control audits, and
- NASA employees involved directly or indirectly with technology are trained in classifying and protecting export-controlled technologies.

After one recommendation was revised, management concurred with the recommendations and stated it was taking action to correct the reported weaknesses. Management plans to develop a catalog of classifications for specific exports, improve training and guidance for Export Control Program auditors, and enhance and strengthen training for NASA employees involved directly or indirectly with technology control.

Ongoing Reviews

Technology Oversight Project.

The Technology Oversight Project (TOP) is a long-term effort to track the advanced technologies developed by NASA. At present, TOP has three major thrusts.

- Tracking developing technologies likely to be used in future communications and space systems, identifying the vulnerabilities of those technologies to exploitation, and developing approaches to counter such exploitation
- Identifying and tracking the exploitation of commercially sensitive technologies
- Identifying and tracking the handling and vulnerability to exploitation of proprietary or trade secret information held by NASA

In concert with the TOP, we are auditing NASA control of sensitive technologies and have initiated an audit of contractor control of sensitive technologies.

Y2K

The Office of Inspector General has identified the Year 2000 computer problem as one of the top 10 challenges to NASA management. We recently issued a report on Year 2000 program oversight of NASA's production contractors, *(Report IG-99-004)* and have three audits underway to assess NASA's efforts to respond to the Year 2000 problem.

X-Vehicle Reviews

The X-33

NASA's X-series space vehicle programs are intended to demonstrate technologies that will contribute to greatly reducing the cost of access to space. NASA, working with industry, is currently developing the X-34 air-launched flight demonstrator, the X-33 advanced technology demonstrator, and the X-38 prototype crew return vehicle.

The NASA OIG is conducting a series of reviews to monitor these innovative programs. We are currently auditing the project management and inspecting the security planning of the X-38. We have already completed assessments of X-33 program security and the X-33's planned use of the Global Positioning System.

The X-34

Infrastructure Protection

Presidential Decision Directive 63 orders the strengthening of the nation's defenses against emerging unconventional threats, including those involving terrorist acts, weapons of mass destruction, assaults on our critical infrastructures, and cyber-based attacks. The NASA OIG is participating on NASA's Critical Infrastructure Protection Team, which is developing a Critical Infrastructure Protection Plan for the Agency in response to the presidential directive.

NASA HQ Computers

The OIG has initiated an inspection of the Headquarters Computer Support Contract. As part of this inspection, we will evaluate contract and subcontract administration, customer service, hardware and software acquisitions and support, and systems security.

Other New Reports

- Implementation of NASA's Integrated Financial Management Project, (Report IG-99-026)
- Commercial Remote Sensing Program Office (Report IG-99-023)
- Home-to-Work Use of Vehicles (Report IG-99-015)
- Hubble Space Telescope Cost Saving Initiatives (Report IG-99-013)
- NAS Data Center General Controls at Ames Research Center, Numerical Aerospace Simulation Facility, (Report IG-99-010)
- Space Station Contingency Planning for International Partners (Report IG-99-009)
- Contractor-Acquired Facilities at Johnson Space Center (Report IG-99-008)

Acquiring OIG Reports

Most reports are posted on the web at www.hq.nasa.gov/office/oig/hq/reports.html
Printed reports can be requested by calling (202) 358-1220